REMARKS

In reply to the Office Action of April 23, 2004, Applicant submits the following remarks. Claims 1, 3, 11-18, 22-25 and 27 have been amended. Claims 30-36 have been added. No new matter has been added. Claims 1-36 are now pending after entry of this amendment. Applicant respectfully requests reconsideration in view of the foregoing amendments and these remarks.

Section 102 Rejections

Claims 1-21 and 24-29 were rejected under 35 U.S.C. 102(b) as allegedly being anticipated by U.S. Patent Number 6,549,626 ("Al-Salqan"). Applicant respectfully disagrees.

Claim 1 recites a method for transmitting a message from a sender to an intended recipient. The method requires encrypting a message using a symmetric key to generate an encrypted message. The encrypted message is sent to an intended recipient without making the symmetric key immediately accessible to the intended recipient. The symmetric key is provided to a third party. If the intended recipient signs and returns to the third party a receipt including a representation of the encrypted message, the third party transfers the receipt to a sender and provides the symmetric key to the intended recipient.

Al-Salqan describes a method for encrypting keys for storage, where the key is a private key or key password, such that the key can be decrypted if the key is lost or unavailable (Abstract, lines 1-3). The key to be encrypted, the key to be used to secure the key to be encrypted and private information of the principal are received as input (col. 3, lines 62-67, col. 4, lines 1-2). A principal's private information, such as the principal's mother's maiden name or social security number, is encoded (column 2, lines 50-52). The encoded result is used to symmetrically encrypt the private key or password (column 2, lines 52-54). The private key or password is again encrypted using the public key of a trusted party, such as a certification authority (column 2, lines 54-57). The result of the two encryptions is a key recovery file that may be stored by the principal or other trusted party (column 2, lines 57-59). When the private key is lost or unavailable, the stored key recovery file can be accessed and decrypted (column 2, lines 59-63). The principal, or another party available to provide the principal's private information, can retrieve the key recovery file and key (column 7, lines 21-26).

Al-Salqan also describes two different types of conventional encryption for maintaining information security, symmetric encryption and asymmetric encryption (column 1, lines 21-60). Symmetric encryption uses the same key to encrypt and decrypt information and can be used when transmitting a message from a sender to a recipient as long as the two have agreed upon the key (*id.*). Asymmetric encryption uses a public key for encryption and a separate, mathematically related private key for decryption (*id.*). The principal shares the public key with those the principal expects will send him or her encrypted messages while maintaining the secrecy of the private key (*id.*). A trusted party, known as a certificate authority, can issue a certificate that binds the public key and identity of the principal so that third parties can verify the identity of the principal (*id.*).

Although Al-Salqan describes the conventional method of sending symmetrically encrypted messages, Al-Salqan does not describe the limitations as required by Applicant's claim 1. Al-Salqan does not describe sending an encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient. In Al-Salqan's description of the conventional method of encrypting the message, the sender and the recipient have agreed upon the key and the recipient therefore has access to the symmetric key. The recipient would therefore have the symmetric key at the time of sending. Further, if the recipient does not have access to the symmetric key at the time of sending, Al-Salqan does not teach a step that prompts a third party to provide the symmetric key to the intended recipient.

In Al-Salqan's description of the method of storing encrypted keys, a key, private information and a key for encrypting the key are input into a system for encoding the key. Al-Salqan does not describe sending an encrypted message to an intended recipient without making the symmetric key immediately available to the intended recipient. The private information that is encoded to symmetrically encrypt the received key must be received by the system performing the encryption. The system therefore has access to the private information.

In addition, there is no receipt including a representation of the encrypted message in either of the described methods in Al-Salqan. Al-Salqan describes a certificate, but the certificate does not include a representation of an encrypted message. The certificate merely allows parties to verify the identity of the principal. The certificate does not include a representation of an encrypted message. Thus, the certificate is not a receipt that is returned to a third party so that the third party transfers the receipt to a sender and provides the symmetric key to an intended recipient.

In summary, Al-Salqan does not suggest or disclose encrypting a message with a symmetric key and sending the message to an intended recipient without making the symmetric key immediately accessible to the recipient. Al-Salqan does not suggest or disclose providing a symmetric key to a third party and providing the symmetric key to the intended recipient if the intended recipient signs and returns a receipt including a representation of an encrypted message to the third party. For at least the foregoing reasons, Applicant submits that claim 1 and its dependent claim 2 are not anticipated by Al-Salqan.

Claim 3 recites a method for transmitting a message from a sender to an intended recipient. The claim requires at a sender, encrypting a message using a symmetric key, encrypting the symmetric key to make the symmetric key accessible to a third party but not immediately accessible to an intended recipient and sending the encrypted message and the encrypted symmetric key to the intended recipient. At the recipient, a receipt including a representation of the encrypted message is signed for the message and the receipt and the encrypted symmetric key are sent to the third party. At the third party, the receipt is transferred to the sender and the symmetric key is provided to the intended recipient if the receipt is properly signed.

The Examiner argues that Al-Salqan discloses the claimed method. However, Applicant submits that Al-Salqan does not disclose signing a receipt as required by claim 3. The Examiner equates the certificate in Al-Salqan to the receipt as required by the claims. As described above, the certificate does not include a representation of an encrypted message. Moreover, even if the certificate were a receipt, a recipient does not send the certificate with an encrypted symmetric message to a third party. In Al-Salqan, the certificate is issued to verify the sender's identity. For at least these reasons, the applicant submits that claim 3 is not anticipated by Al-Salqan.

Claim 4 recites a method for certifying receipt of a message. The claim requires that a signed receipt and an encrypted symmetric key are received from an intended recipient, where the signed receipt memorializes receipt of the encrypted message by the intended recipient. Al-Salqan describes a certificate authority that issues a certificate which allows third parties to verify the identity of the principal. The certificate does not memorialize receipt of an encrypted message by an intended recipient. The certificate is not a signed receipt as required by claim 4 and for at least this reason, Applicant submits that claim 4 is not anticipated by Al-Salqan.

Claim 5 recites a method for certifying receipt of a message sent from a sender to an intended recipient. The method includes receiving a separately encrypted message header associated with the message. Al-Salqan does not suggest or suggest or disclose receiving a separately encrypted message header associated with the message. For at least this reason, Applicant submits that claim 5 is not anticipated by Al-Salqan

Claim 6 recites a method including receiving from a third party a certified receipt that is verified by the third party and indicates that an intended recipient received a message where the message was encrypted using a symmetric key. Although Al-Salqan teaches a certificate, the certificate does not indicate that an intended recipient received a message. For at least this reason, Applicant submits that claim 6 is not anticipated by Al-Salqan.

Claim 7 recites a method including creating a message header that includes a symmetric key and a message identifier associated with a message, encrypting the message with the symmetric key, encrypting the message header with a public key of a third party and attaching the message header to the encrypted message forming a certified message that is forwarded to an intended recipient. A certified receipt from the intended recipient that has been verified at the recipient is received and forwarded to a sender after verification. The validity of the receipt is verified using the stored symmetric key and the certified message.

Al-Salqan does not disclose or suggest at least the step of creating a message header that includes a symmetric key and a message identifier associated with the message. For at least this reason, claim 7 is not anticipated by Al-Salqan.

Claim 8 recites a method for providing a receipt for a message including creating a receipt for an encrypted message, including signing a hash of an encrypted message and returning the signed receipt to a third party. After verification of the signed receipt at the third party, the symmetric key is received from the third party.

As stated above, Al-Salqan describes a certificate authority that can issue a certificate linking a principal to a public key. However, issuing a certificate does not include providing a receipt for an encrypted message that includes a signed hash of the encrypted message. Further, issuing a certificate does not include receiving a symmetric key from a third party where the third party was sent the signed receipt. For at least these reasons, Applicant submits that claim 8 is not anticipated by Al-Salqan. Claim 9 depends from claim 8 and is similarly not anticipated.

Amended claim 11 recites a method that requires receiving a message encrypted by a symmetric key and receiving a hash of the symmetric key. A representation of the hash of the symmetric key and the message encrypted by the symmetric key are generated so that a message identifier is generated. The message identifier is generated prior to decrypting the message. The message identifier is used to verify receipt of the message at the intended recipient without exposing the message content.

Although Al-Salqan teaches encoding the personal information, such as by hashing, and using the encoded version of the personal information as a symmetric key and encrypting the encrypted key with a public key, Al-Salqan does not disclose or suggest hashing the symmetric key, much less generating a message identifier by generating a representation of a hash of the symmetric key and the message encrypted by the symmetric key. Further, Al-Salqan does not teach a message identifier that is used to verify receipt of the message at the intended recipient without exposing the message content. For at least this reason, Applicant submits that claim 11 and claims 12-16, which depend from claim 11, are not anticipated by Al-Salqan.

Amended claim 17 recites a method including receiving a message encrypted by a symmetric key and receiving a hash of the symmetric key. A representation of the hash of the symmetric key and the message encrypted by the symmetric key is generated. The representation is signed to generate a signed receipt, where the receipt is generated prior to decrypting the message and receiving the symmetric key.

As stated above, Al-Salqan describes encrypting messages with keys and encrypting keys for storage, but does not teach or suggest generating a representation of a hash of a symmetric key and a message encrypted by the symmetric key and signing the representation. For at least this reason, Applicant submits that claim 17 and claims 18 and 19, which depend from claim 17, are similarly not anticipated.

Claims 20-21 and 24-29 each require time stamping a representation. Al-Salqan does not suggest or disclose using a time stamp or time-stamping. For at least this reason, Applicant submits that claims 20-21 and 24-29 are not anticipated.

Claim Objections

Claims 22 and 23 were objected to as being based on a rejected claim, but would be allowable if rewritten in independent form. Claims 22 and 23 have been amended to include the limitations of the claims upon which they depend. Applicant believes these claims are now in condition for allowance.

New Claims

Claims 30-36 are new. No new matter has been added. Claim 30 depends from claim 1. Claims 31 is independent and claims 32-33 depend from claim 31. Applicant asserts that claims 31-33 are not anticipated by Al-Salqan. Claims 34 and 36 are new independent claims, which the applicant asserts is not anticipated by Al-Salqan.

Please apply the Request for Continued Examination fee of $375, the One-Month Extension of Time fee of $55, excess claim fees of $278, and any other appropriate charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: Aug 18, 2004

Jennifer A. Zarocco
Reg. No. 54,563

Customer No.: 26181
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50212723.doc